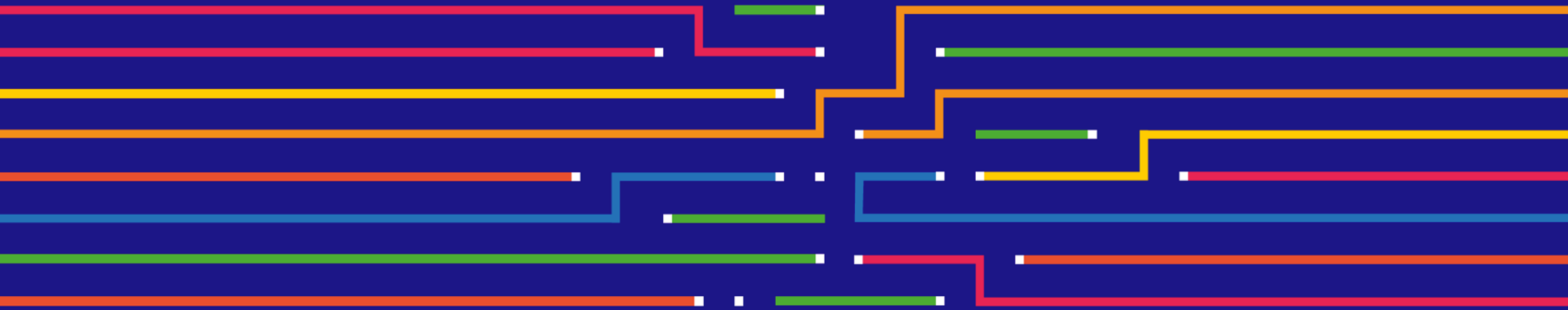


RedCLARA
Cooperación Latino Americana de Redes Avanzadas

IMPLEMENTING ROUTING SECURITY

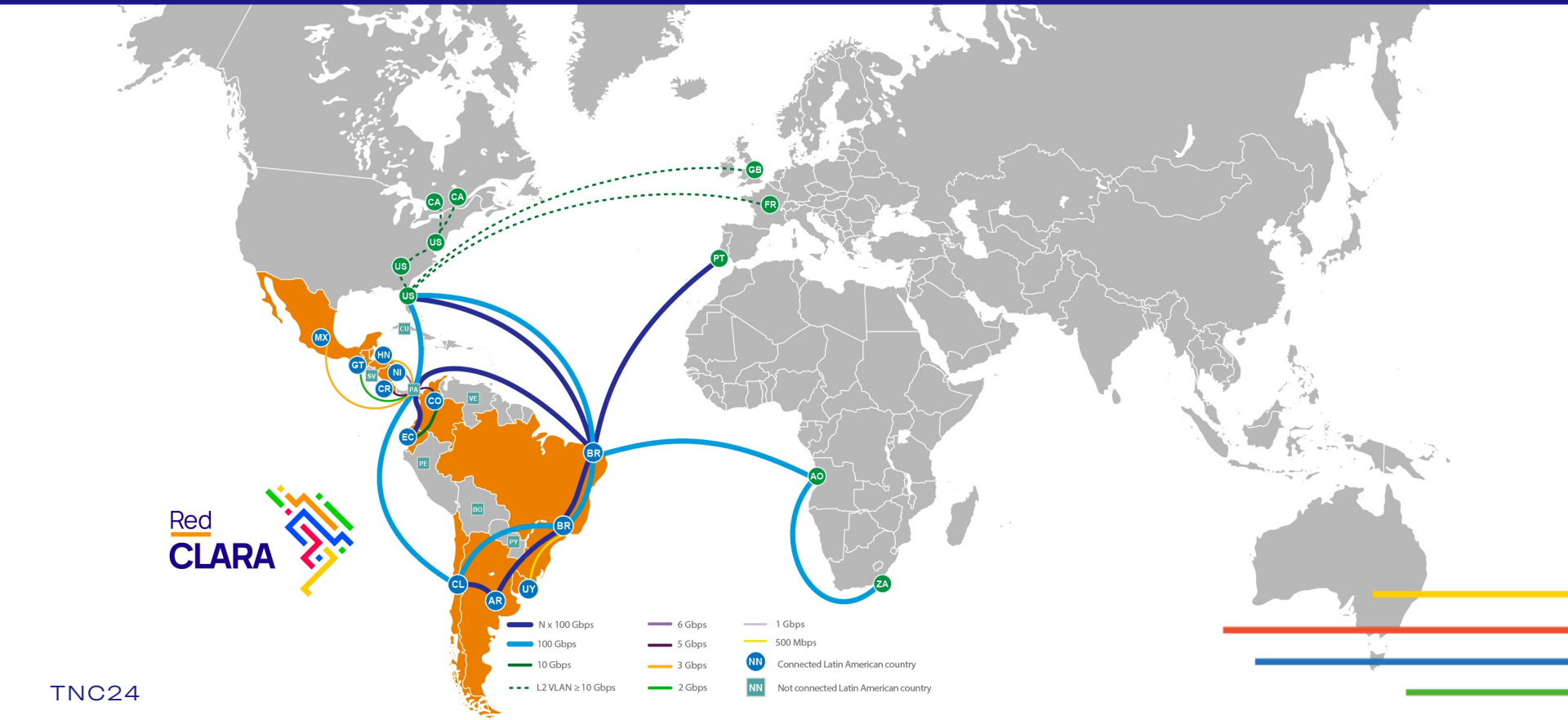
for Latin American and European NRENs

Tiago Monsores, Lead Network Engineer

Introduction

RedCLARA
Cooperación Latino Americana
de Redes Avanzadas

RedCLARA is responsible for the implementation and management of the network infrastructure that interconnects the Latin American National Research and Education Networks (NRENs), and through them, a large number of universities and research centers.


GB
FR
CA
CA
US
US
US
PT
MX
CU
HN
GT
SV
NI
CR
PA
CO
VE
EC
PE
BR
AO
BO
BR
PY
CL
AR
UY
ZA
Red
CLARA
N x 100 Gbps
100 Gbps
10 Gbps
L2 VLAN ≥ 10 Gbps
6 Gbps
5 Gbps
3 Gbps
2 Gbps
1 Gbps
500 Mbps
NN
Connected Latin American country
NN
Not connected Latin American country

Members

RNP

cedia

REUNA
Ciencia y Educación en Red

RENATA
COLOMBIA

InnovaRed
Red Nacional de Investigación y Educación de Argentina

RAU
RED ACADÉMICA URUGUAYA

CONARE

ragie

cudi

- Currently RedCLARA has 9 associated members
- The coverage area is 15.76 million km²
- For comparison, Europe area is 10.18 million km²
- +105,435 km of network circuits
- +3,059 PB of transmitted data in 2023
- +2,000 connected universities

Infrastructure

Cisco ASR 9904

- 6 RU
- Up to 16 Tbps
- 2 line cards, 2 RSPs

Ciena WaveServer Ai

- 1 RU
- Up to 2.4 Tbps line + 2.4 client
- 3 transponder slots

NEG Systems

Grafana
Network traffic monitoring

chronograf
Virtual machines monitoring

graylog
Management of log messages

ElastiFlow
Collects and analyzes network flows

Oxidized
Configuration backup and management

ZABBIX
Monitoring and alerting system

Pushover
Push notifications system

TACACSGUI
User authetication, and command authorization and accounting

ROUTINATOR
RPKI validation system

INTEGRATED MONITORING PORTAL
Integrated Monitoring Portal

netbox
Network assets inventory system

FASTNETMON
DDoS attacks detection and mitigation

What is MANRS?

MANRS

MANRS – Mutually Agreed Norms for Routing Security – is a global initiative created in 2014 with the support of the Internet Society and with the goal of improving the security and resilience of the global routing system based on a list of recommendations.

What is MANRS?

MANRS

The list of recommendations includes:

1. Preventing propagation of incorrect routing information;
2. Preventing traffic with spoofed source IP address (anti-spoofing);
3. Facilitating communication and coordination between network operators;
4. Facilitating validation of routing information on a global scale (RPKI).

How are we?

RedCLARA
Cooperación Latino Americana de Redes Avanzadas

RedCLARA is a MANRS participant and has successfully implemented all 4 recommended actions:

- ✓ Action 1: Filtering
- ✓ Action 2: Anti-Spoofing
- ✓ Action 3: Coordination
- ✓ Action 4: Global Validation

How are we?

- 3 NRENs are MANRS participants
  - ✓ RNP
  - ✓ CONARE
  - ✓ CEDIA
- 6 NRENs are not MANRS participants

How are we?

RNP cedia REUNA Ciencia y Educación en Red

RENATA COLOMBIA InnovaRed Red Nacional de Investigación y Educación de Argentina RAU RED ACADÉMICA URUGUAYA

CONARE ragie cudi

Starting in July 2023, the MANRS compliance score was made public to all participants.

This change has been made by the MANRS Steering Committee and is intended to align objectives of the community for the following points:

How are we?

RNP cedia REUNA Ciencia y Educación en Red

RENATA COLOMBIA InnovaRed Red Nacional de Investigación y Educación de Argentina RAU RED ACADÉMICA URUGUAYA

CONARE ragie cudi

- Raise awareness of routing security problems and encourage networks to implement best current practices to address them.
- Improve transparency and credibility of the MANRS initiative.
- Promote a culture of collective responsibility toward the security and resilience of the Internet's global routing system.

Organization Name	Date Approved	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Routing Information	
							IRR	RPKI
RedCLARA	19th Jan 2022	AR, BR, CL, CO, CR, EC, GT, HN, MX, NI, UY	27750	✓	100%	100%	100%	100%
Rede Nacional de Ensino e Pesquisa	11th Dec 2019	BR	1916	✓		100%	99%	91%
CONARE	1st Apr 2020	CR	52470	✓		100%	100%	100%
CEDIA	6th Jul 2020	EC	61468, 27841, 27820, 262212	✓	No data	100%	100%	99%

Data last measured: 1st May 2024

Source: https://www.manrs.org/netops/participants/

Organization Name	Date Approved	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Routing Information	
							IRR	RPKI
GÉANT	25th Aug 2018	EU	21320, 20965	✓	No data	100%	100%	100%
ACOnet	2nd Jul 2019	AT	1853	✓		100%	100%	26%
SWITCH	25th Aug 2018	CH	559	✓	No data	100%	100%	82%
DFN-Verein	6th Jul 2020	DE	680	✓	No data	100%	100%	68%
NORDUnet	25th Aug 2018	DK, FI, IS, NO, SE	2603	✓	No data	100%	92%	85%
RedIRIS	25th Aug 2018	ES	766	✓	No data	100%	97%	35%
GRNET	25th Aug 2018	GR	5408	✓	No data	100%	100%	76%

Data last measured: 1st May 2024

Source: https://www.manrs.org/netops/participants/

Organization Name	Date Approved	Areas Served	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Routing Information	
							IRR	RPKI
HEAnet	19th May 2022	IE	1213	✓	No data	100%	100%	94%
GARR	20th Jul 2020	IT	137	✓	No data	100%	100%	80%
Fondation RESTENA	22nd Oct 2018	LU	2602	✓	No data	100%	100%	86%
SURF	25th Aug 2018	NL	1103	✓	100%	100%	100%	86%
FCCN	13th Nov 2023	PT	1930	✓	100%	100%	100%	100%
Agency ARNIEC - RoEduNet	16th Feb 2021	RO	2614	✓	100%	100%	99%	10%
URAN Association	2nd Jun 2020	UA	12687	✓		100%	100%	100%

Data last measured: 1st May 2024

Source: https://www.manrs.org/netops/participants/

How to implement MANRS in 100%?

Action 1 : Filtering

- Preventing the spread of incorrect routing information
- The simplest way is through the use of prefix-list for the routes received from BGP neighbors

```
router bgp 27750
 vrf INTERNET
  neighbor 200.0.204.245
   remote-as 52470
   description CONARE Internet
   address-family ipv4 unicast
    route-policy CONARE-INTERNET-IN in
    route-policy CONARE-INTERNET-OUT out
    remove-private-AS
   !
  !
 !
!
route-policy CONARE-INTERNET-IN
  if destination in CONARE.INTERNET then
    set community (27750:64104)
  else
    drop
  endif
  if validation-state is invalid then
    set local-preference -10
  endif
end-policy
!
```

```
route-policy CONARE-INTERNET-OUT
  if destination in DEFAULT then
    done
  else
    drop
  endif
end-policy
!
prefix-set CONARE.INTERNET
  179.0.20.0/22 le 24
end-set
!
```

How to implement MANRS in 100%?

Action 2 : Anti-Spoofing

- Preventing traffic with illegitimate IP addresses of origin
- There are many ways to do it but the recommended one is using the protocol called uRPF

How to implement MANRS in 100%?

Action 2 : Anti-Spoofing

uRPF has 2 different algorithms:

- uRPF loose
- uRPF strict

The protocol must be configured on the input and output interfaces of the network

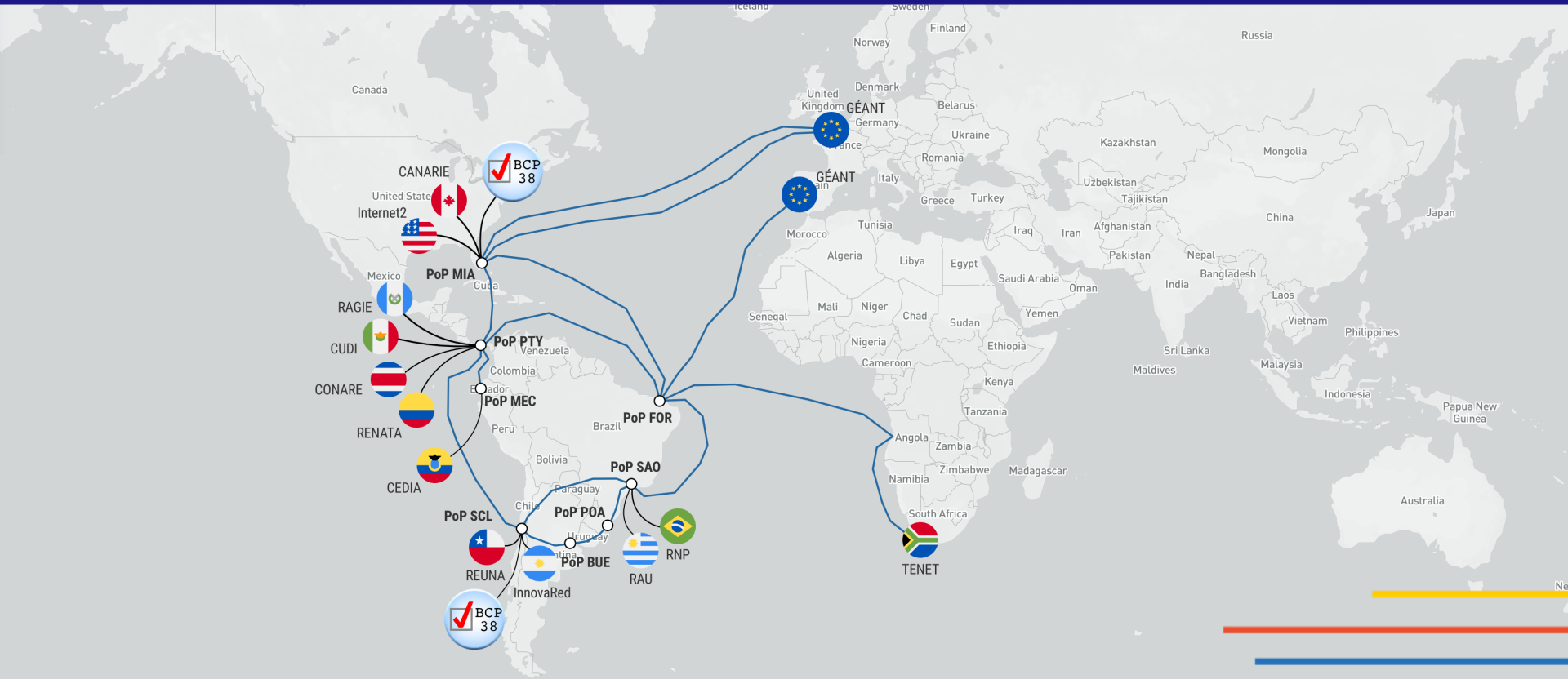
```
RP/0/RSP0/CPU0:rtr-core-pty(config-subif)#ipv4 verify unicast source reachable-via ?
  any  Source is reachable via any interface
  rx   Source is reachable via interface on which packet was received


interface Bundle-Ether1.55
 description CONARE Internet
 mtu 1522
 vrf INTERNET
 ipv4 address 200.0.204.244 255.255.255.254
 ipv4 verify unicast source reachable-via any allow-self-ping allow-default
 ipv6 verify unicast source reachable-via any allow-self-ping allow-default
 ipv6 address 2001:1348:1:7::34/127
 flow ipv4 monitor FLOW-MONITOR-MAP-IPv4 sampler SAMPLER-MAP-1-OUT-OF-10000 ingress
 flow ipv6 monitor FLOW-MONITOR-MAP-IPv6 sampler SAMPLER-MAP-1-OUT-OF-10000 ingress
 encapsulation dot1q 1506 second-dot1q 55
!
```

How to implement MANRS in 100%?

Action 2 : Anti-Spoofing

- For BCP38 validation tests, we must install CAIDA Spoofer application in 2 different points of the network
- The results are verified regularly and published on the CAIDA website.


Canada
United States
Mexico
Cuba
Venezuela
Colombia
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Uruguay
Argentina
Iceland
Sweden
Finland
Norway
Russia
Denmark
United Kingdom
Germany
France
Belarus
Ukraine
Romania
Italy
Spain
Greece
Turkey
Kazakhstan
Mongolia
Uzbekistan
Tajikistan
China
Japan
Afghanistan
Iran
Iraq
Pakistan
Nepal
Bangladesh
India
Tunisia
Morocco
Algeria
Libya
Egypt
Saudi Arabia
Oman
Yemen
Laos
Vietnam
Philippines
Sri Lanka
Malaysia
Maldives
Indonesia
Papua New Guinea
Australia
Senegal
Mali
Niger
Chad
Sudan
Nigeria
Cameroon
Ethiopia
Kenya
Tanzania
Angola
Zambia
Zimbabwe
Namibia
Madagascar
South Africa
CANARIE
BCP 38
Internet2
PoP MIA
RAGIE
CUDI
CONARE
RENATA
CEDIA
PoP PTY
PoP MEC
PoP FOR
PoP SAO
PoP SCL
PoP POA
PoP BUE
REUNA
InnovaRed
RAU
RNP
BCP 38
GÉANT
GÉANT
TENET

ASRank About Ranking Search Contact Data FAQ Feedback
AS 27750: neighbors

27750 search

AS number	27750
AS name	unknown
organization	Cooperación Latino Americana de Redes Avanzadas
country	Uruguay
AS rank	599
customer cone	67 asn, 918 prefix, 840128 address
AS degree	15 global, 14 transit, 4 provider, 3 peer, 8 customer

Correction

Spoofer 06/2023-06/2024		
Tested IP Blocks	2	1
Spoofing IP Blocks	0 (0.0%) IPv4 /24s	0 (0.0%) IPv6 /40s

see more spoofer data >

How to implement MANRS in 100%?

Action 3 : Coordination

- Facilitating global operational communication and coordination between network operators
- Network operators are expected to keep contact information up-to-date and globally accessible

How to implement MANRS in 100%?

Action 3 : Coordination

- In the RIR portal the aut-num, route, route6 and as-set objects must be created and updated
- In PeeringDB the AS and contact information must be updated. IRR as-set is very important
- Information in RADb is desirable, but optional

```
[tmonsores@home ~]$ whois as27750

aut-num:     AS27750
owner:       Cooperación Latino Americana de Redes
Avanzadas
ownerid:     UY-CLAR-LACNIC
responsible: Luis Eliécer Cadenas Marín
address:     Rambla Republica de Mexico, 6125,
address:     11200 - Montevideo -
country:     UY
phone:       +598 2 6042222 [5301]
owner-c:     MAT144
routing-c:   MAT144
abuse-c:     MAT144
created:     20040707
changed:     20190814

nic-hdl:     MAT144
person:      Marco Teixeira
e-mail:      marco.teixeira@redclara.net
address:     Hermantino Coelho, 77, -
address:     - - Campinas -
country:     BR
phone:       +55 19 37873367 [0000]
created:     20190226
changed:     20220112
```

PeeringDB

Search here for a network, IX, or facility.

Advanced Search Legacy Search

Registeror Login

English (English)

Cooperación Latino Americana de Redes Avanzadas

Organization	Cooperación Latino Americana de Redes Avanzadas
Also Known As	RedCLARA
Long Name	
Company Website	http://www.redclara.net
ASN	27750
IRR as-set/route-set	AS27750:AS-MEMBERS
Route Server URL	
Looking Glass URL	
Network Type	Educational/Research
IPv4 Prefixes	1500
IPv6 Prefixes	250
Traffic Levels	Not Disclosed
Traffic Ratios	Not Disclosed
Geographic Scope	Not Disclosed
Protocols Supported	⊘ Unicast IPv4 ○ Multicast ⊘ IPv6 ○ Never via route servers
Last Updated	2022-07-27T05:33:55Z
Public Peering Info Updated	
Peering Facility Info Updated	2019-04-16T13:24:56Z
Contact Info Updated	2019-04-15T13:37:27Z
Notes	
RIR Status	ok
RIR Status Updated	2022-07-27T05:29:57

Public Peering Exchange Points

Filter

Exchange AŻ / IPv4	ASN / IPv6	Speed	RS Peer

No filter matches.
You may filter by **Exchange**, **ASN** or **Speed.**

Interconnection Facilities

Filter

Facility AŻ / ASN	Country / City
Equinix MI1 - Miami, NOTA	United States of America
27750	Miami
Equinix SP4 - São Paulo	Brazil
27750	Barueri

How to implement MANRS in 100%?

Action 4 : Global validation

- All objects discussed in action 3 are expected to be properly created
- An RPKI validation system must be implemented and connected to the routers
- A routing policy should be applied decreasing the priority of invalid routes

ROUTINATOR

Prefix Check | Metrics | Repositories | Connections

Prefix or IP Address

e.g. 192.0.2.0/24

Origin ASN (optional)

e.g. 64511

will be validated with BGP ASN

Validate hide options

ASN Lookup

Validate Prefixes for ASN found in BGP

Origin ASN Validation Source

Longest Matching Prefix Exact Match only

Data Freshness

RPKI	2024-06-04 23:30:15 UTC (1 hour ago)
BGP	2024-06-04 18:06:11 UTC (6 hours ago)
RIR	2024-06-04 0:06:42 UTC - 2024-06-04 22:12:29 UTC (2 hours ago)

```
router bgp 27750
 rpki server 138.59.12.91
  bind-source interface Loopback0
  transport tcp port 3323
  response-time 300
 !
 address-family ipv4 unicast
  bgp origin-as validation enable
 !
 address-family ipv6 unicast
  bgp origin-as validation enable
 !
 vrf LHCONE
  address-family ipv4 unicast
   bgp origin-as validation enable
  !
  address-family ipv6 unicast
   bgp origin-as validation enable
  !
```

```
vrf INTERNET
  address-family ipv4 unicast
   bgp origin-as validation enable
  !
  address-family ipv6 unicast
   bgp origin-as validation enable
  !
 vrf COPERNICUS
  address-family ipv4 unicast
   bgp origin-as validation enable
  !
  address-family ipv6 unicast
   bgp origin-as validation enable
  !
 vrf AcdContinental
  address-family ipv4 unicast
   bgp origin-as validation enable
  !
  address-family ipv6 unicast
   bgp origin-as validation enable
```

```
router bgp 27750
 vrf INTERNET
  neighbor 200.0.204.245
   remote-as 52470
   description CONARE Internet
   address-family ipv4 unicast
    route-policy CONARE-INTERNET-IN in
    route-policy CONARE-INTERNET-OUT out
    remove-private-AS
   !
  !
 !
!
route-policy CONARE-INTERNET-IN
  if destination in CONARE.INTERNET then
    set community (27750:64104)
  else
    drop
  endif
  if validation-state is invalid then
    set local-preference -10
  endif
end-policy
!
```

```
route-policy CONARE-INTERNET-OUT
  if destination in DEFAULT then
    done
  else
    drop
  endif
end-policy
!
prefix-set CONARE.INTERNET
  179.0.20.0/22 le 24
end-set
!
```

How to implement MANRS in 100%?

Action 4 : Global validation

Recommended websites:

- Routinator: https://github.com/NLnetLabs/routinator
- IRR Explorer: https://irrexplorer.nlnog.net

IRR EXPLORER

Prefix, IP, ASN or AS-set

Search

Data source status

Reduced colour mode

Report for ASN AS27750

What does the prefix table show?

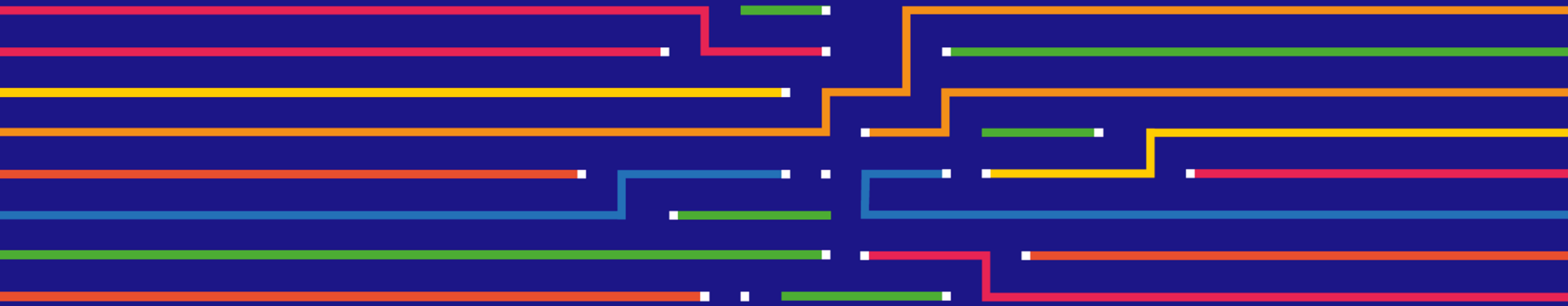
Explanation of different messages

Prefixes originated by AS27750

Prefix	RIR	BGP	RPKI	LACNIC	RADB	Advice
138.59.12.0/22	LACNIC	27750	27750 /22	27750	27750	Everything looks good
200.0.204.0/22	LACNIC	27750	27750 /22	27750	27750	Everything looks good
2001:1348::/32	LACNIC	27750	27750 /32	27750		Everything looks good

Source data as JSON

¿QUESTIONS?



RedCLARA
Cooperación Latino Americana de Redes Avanzadas

redclara.net
tiago.monsores@redclara.net
linkedin.com/in/tiagomonsores